UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/650,105	08/29/2000	Baskaran Dharmarajan	MSFT115431	9027

26389 7590 02/15/2005

CHRISTENSEN, O'CONNOR, JOHNSON, KINDNESS, PLLC
1420 FIFTH AVENUE
SUITE 2800
SEATTLE, WA 98101-2347

EXAMINER	
ARANI, TAGHI T	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 02/15/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/650,105	DHARMARAJAN, BASKARAN	
	Examiner	Art Unit	
	Taghi T. Arani	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 June 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 are presented for examination.

Response to Amendment

2. Applicant's arguments filed 6/30/2004 regarding the rejection of the claims 1-21 under 35 U.S.C. 103(a) have been fully considered but they are not persuasive.

As per Applicant's arguments relating to the rejections of claims 1,13 and the primary reference of Sasmazel, the Applicant argues that "Sasmazel does not disclose a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application:" and that "Sasmazel discloses a system where authentication is not connected to a specific computer. Instead, authentication is tied to an application such as a web server that is distributed among multiple computers". Applicant further argues "the present invention authorizes users to access multiple server-based applications that may or may not be located on different computers. Thus, the present invention is not limited to authorizing a user to access a specific application", page 13, second paragraph of REMARKS.

The Examiner responds that Sasmazel expressly discloses (see abstract, see also col. 8, lines 41-58) an eticket architecture generated by an authentication server that may then be transmitted over the Internet from server to server (i.e. server-based application) without having the information in the eticket altered, and without having to re-authenticate the user at each server (multiple server-based application is inherent) . That is, the teaching of Sasmazel suggests that once an eticket is generated for a user of a computer, then the user is authorized to access

second second-based application based upon previously provided authorization (by provision of eticket) to access a first server-based application.

As per applicant's argument relating to the Blaze's reference, the Applicant argues that " storing time and date information related to the use of smartcard is not the same as determining a session length that indicates a length of time a user is authorized to access a server-based application", page 15 of REMARKS.

The Examiner responds that as stated in the rejection of claims 1, 10 and 13 in previous office action and below, Blaze does disclose that the smartcard stores in a field of activity storage area the length of time during which the escrow agent has access to the encrypted file system (col. 7, lines 1-14) .

As per Applicant's argument relating to Misra's reference, the Applicant sates that he is unable to find in Misra a time counter or any other mechanism for determining a session length.

The Examiner responds that Misar teaches (col. 7, lines 44-46) that the time stamp helps to minimize the time period in which an eavesdropper may use a copied ticket (which includes session key) and authenticator pair. This suggests a time counter for determining session length based on a value of an elapsed time counter.

As per applicant's arguments relating to

Applicant further arguments relating to the rejection of dependent claims 2-9, 11-12, 14-21 are based on the presumed allowability of base claims 1 and 13.

The Examiner responds that dependent claims 2-9, 11-12, 14-21 stand rejected based on rejected base claims 1, 10 and 13 and the statements of rejections of claims 2-9, 11-12, 14-21 provided in the previous office action and below.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-5, 8, 13 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over prior art of record, Sasmazel et al. (U.S. Patent 6,263,432 and Sasmazel hereinafter) in view of Blaze (U.S Patent 5,721,777) in view of Roberts et al. (U.S. Patent 6,101,486 and Roberts hereinafter) in further view of Misra et al. (U.S. Patent 5,999,71 1 and Misra hereinafter).

In regards to claim 1, Sasmazel teaches a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application (col. 1, lines 9- 11) (col. 7, lines 44-45), comprising:

(a) receiving a request to access said second server-based application (i.e. a user requests a function from either server 220 or 240) (col. 10, lines 20-22);

(b) in response to said request,

(ii) calculating a hash value for an authorization ticket received from said first server-based application (i.e. authentication server) (col. 7, lines 50-57), and

(iii) transmitting a request for authorization to said second server-based application comprising said hash value and said authorization ticket (col. 9, lines 64-67), (col. 10, lines 20-23).

Sasmazel does not teach:

* determining a session length indicating a length of time said client

computer has been authorized to access said first server-based application,

* including a shared secret in the authentication ticket; and

* including the computed session length with the authentication ticket

Blaze discloses a system for accessing encrypted data with portable cryptographic modules (col. 1, lines 7-8).

Blaze teaches that once a smartcard (i.e. client) is deemed valid (i.e. a session is started), the smartcard may be used to decrypt on or more files stored in the system (col. 6, lines 44-46). The smartcard uses a clock to start a timer, ascertain the data and time at which the file decryption occurred, and store such time and date in appropriate fields (col. 6, lines 57-5%. The smartcard stores in a field of activity storage area the length of time during which the escrow agent had access to the encrypted file system (col. 7, lines 1-4).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sasmazel with the teachings of Blaze to include determining a session length indicating a length of time said client computer has been authorized to access said first server-based application with the motivation to allow authorized parties to determine the use of the module and the duration of such use (Blaze, col. 2, lines 34-36).

Roberts discloses a system that relates to the field of Internet communications (col. 1, lines 6-7).

Roberts teaches that when a customer accesses a company's website, information about the customer is gathered and stored in a "cookie" (i.e. ticket). This cookie may log the customer's active input operations as well as the customer's passive activity (i.e., time spent viewing a particular webpage, etc.) (col. 5, lines 2-24). The Office infers that the time spent

viewing a particular webpage is substantially similar to the session length.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sasmazel and Blaze with the teachings of Roberts to include the computed session length within the authentication ticket with the motivation to allow greater and more readily available access to a customer's information and preferences (Roberts, col. 2, lines 17-19).

Misra discloses a system that relates to the use of logon certificates in a distributed system (col. 1, lines 7-10).

Misra teaches including a session key (i.e. shared secret) within a logon certificate (i.e. authentication ticket) (figure 2A).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sasmazel, Blaze and Roberts with the teachings of Misra to include a shared secret (i.e. session key) within the authentication ticket with the motivation to provide a secure and efficient approach for supporting roaming users (Misra, col. 3, lines 65-67). In regards to claim 2, Sasmazel does not teach that the authorization ticket comprises a time stamp, and that determining a session length comprises subtracting said time stamp from an elapsed time counter to determine said session length.

Misra teaches that the authorization ticket comprises a time stamp (col. 7, lines 44-46). The Examiner takes Official Notice that computing a session length by subtracting a time stnmp from an elapsed time counter is old and well known in the art.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Blaze, Roberts and Misra with the teachings

of Misra to include a timestamp within the authorization ticket and computing a session length by subtracting a timestamp from an elapsed time counter with the motivation to minimize the time period in which an eavesdropper may use a copied ticket (Misra, col. 7, lines 48-40).
In regards to claim 3, Blaze teaches that the elapsed time counter is started when said authorization ticket is received from said first server-based application (i.e. once the smartcard is deemed valid) (col. 6, lines 44-67).

In regards to claim 4, Sasmazel teaches that the ticket is received from the first server-based application when the client computer is authorized to access that first server-based application (col. 10, lines 9-20).

In regards to claim 5, Sasmazel teaches that calculating a hash value comprises performing an MD5 hash of an authorization ticket received from said first server-based application, said session length, and a secret shared between said client computer and said second server-based application (col. 2, lines 41-42).

In regards to claim 8, Sasmazel teaches that the first server-based application comprises an instant messaging server computer (i.e. web server) and that the second server-based application comprises a Web server computer (figure 2).

In regards to claim 13, Sasmazel teaches a method for authorizing a client computer to access a second server-based application based upon previously provided authorization to access a first server-based application (col. 1, lines 9-1 1) (col. 7, lines 44-45), comprising:

(a) receiving a request for authorization to access said second server-based application from said client computer (figure 7, path V4) comprising a hash value (figure 4, #306), and an authorization ticket (figure 4, # 302 and 304);

(b) computing a new hash value for said authorization ticket (col. 8, lines 60-61),

(c) determining whether said hash value received from said client computer is identical to said new hash value (col. 8, lines 65-67); and

(d) in response to determining that said hash value received from said client computer is identical to said new hash value, authorizing said client computer to access said second server-based application (col. 9, lines 10-12).

Sasmazel does not teach:

* Including a session length in the request for authorization.

* Computing a hash for the authorization ticket, session length and a copy of a secret shared between the client computer and the second server-based applications.

Roberts teaches that when a customer accesses a company's website, information about the customer is gathered and stored in a "cookie" (i.e. ticket). This cookie may log the customer's active input operations as well as the customer's passive activity (i.e., time spent viewing a particular webpage, etc.) (col. 5, lines 2-24). The Office infers that the time spent viewing a paricular webpage is substantially similar to the session length.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sasmazel with the teachings of Roberts to include a session length in the request for authorization (i.e. cookie) with the motivation to allow greater and more readily available access to a customer's information and preferences (Roberts, col. 2, lines 17-19).

Misra teaches including a session key (i.e. shared secret) within a logon certificate (i.e.

authentication ticket) (figure 2A).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to modify the system of Sasmazel and Roberts with the teachings of Misra to include a shared secret (i.e. session key) within the authentication ticket with the motivation to provide a secure and efficient approach for supporting roaming users (Misra, col. 3, lines 65-67).

The resulting authentication ticket would then be comprised of the original authentication ticket, the session length and the session key. Therefore, the hash performed by Sasmazel on the authentication ticket would be a hash of the original authorization ticket, the session length, and a secret shared between the client computer and the second server-based application.

In regards to claim 17, the claim limitation recites a computer-controlled apparatus operative to perform the method of claim 13, therefore the same rejection applies.

In regards to claim 19, the claim limitation recites a computer-readable medium containing computer-readable instructions which, when executed by a computer, perform the method of Claim 13, therefore the same rejection applies.

3. **Claims 6-7** are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasmazel in view of Blaze in view of Roberts in view of Misra as applied to claim 1 above, in further view of Wang et al. (U.S. Patent 6,005,853 and Wang hereinafter).

In regards to claim 6, the system of Sasmazel, Blaze, Roberts and Misra teaches the system of claim 1 as discussed above.

The system of Sasmazel, Blaze, Roberts and Misra does not teach further comprising: starting a persistence timer; determining whether the persistence timer has reached a predefined

value prior to receiving a response from the second server-based application', and in response to determining that the persistence time has reached a predefined value prior to receiving a response from the second server-based application, deleting the authorization ticket, the session length and the hash value from the client computer.

Wang discloses a network access scheme (col. 3, lines 3-4).

Wang teaches that when a data packet (i.e. authentication ticket) is sent, a sequence variable is allocated and an acknowledgement timer (i.e. persistence timer) is set to prevent waiting indefinitely. When the acknowledgement timer times out and the number of retries has been exhausted, the machine deletes the sequence variable and returns to the idle state (col. 11, lines 6-50). The sequence variable of Wang is analogous to the authorization ticket, the session length and the hash value of the instant invention.

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Blaze, Roberts and Misra with the teachings of Wang to include starting a persistence timer; determining whether the persistence timer has reached a predefined value prior to receiving a response from the second server-based application; and in response to determining that the persistence time has reached a predefined value prior to receiving a response from the second server-based application, deleting the authorization ticket, the session length and the hash value from the client computer with the motivation to prevent waiting indefinitely (Wang, col. 11, lines 21-22).

In regards to claim 7, the system of Sasmazel, Blaze, Roberts and Misra does not teach that in response to determining that the persistence timer has not reached a predefined value prior

to receiving a response from said second server-based application, receiving the response from the second server-based application and displaying the response at said client computer.

Wang teaches that in response to determining that the persistence timer has not reached a predefined value prior to receiving a response (i.e. acknowledgment package) from said second computer, receiving the response from the second server-based application and displaying the response (i.e. returning to the idle state) at said client computer (col. 11, lines 6-50)

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Blaze, Roberts and Misra with the teachings of Wang to include that in response to determining that the persistence timer has not reached a predefined value prior to receiving a response from said second server-based application, receiving the response, from the second server-based application and displaying the response at said client computer with the motivation to prevent waiting indefinitely (Wang, col. 11, lines 21 22).

4. **Claims 14-16, 18, 20-21** are rejected under 35 U.S.C. 103(a) as being unpatentable over Sasmazel et al. in view of Roberts in view of Misra as applied to claim 13 above, in further view of Hershey et al. (U.S. Patent 5,48 1,53%.

In regards to claim 14, the combination of Sasmazel, Roberts and Misra teaches the system of claim 13 as discussed above.

The combination of Sasmazel, Roberts and Misra does not teach that in:

(e) in response to determining that the hash value received from the client computer is identical to the new hash value,

(i) determining whether a sum of the session length and a time stamp received as part of

the authorization ticket is within a preset threshold value of a current time, and

(ii) in response to determining that the sum of the session length and the time stamp is within a preset threshold value, authorizing the client computer to access said second server-based application.

Misra teaches that the authorization ticket comprises a time stamp (col. 7, lines 44-46).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Roberts and Misra with the teachings of Misra to include a timestamp within the authorization ticket with the motivation to minimize the time period in which an eavesdropper may use a copied ticket (Misra, col. 7, lines 40-50).

Hershey discloses a system that relates to the field of digital message transmission (col. 1, lines 20-21).

Hershey teaches that a unit (i.e. client computer) will try to send a message packet (i.e. ticket) to a number of receivers (i.e. web servers) before the message expires, and that it determines whether a message expires by adding a "LIFETIME" (i.e. session length) value to a "TIMESTAMP" value in the message packet. This message is then compared to the current time to determine whether the message expired or not. If the message has not expired, then the message packet is rebroadcast and the remaining steps are performed (i.e. authorization continues as normal) (col. 7, lines 34-43)

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Roberts and Misra with the teachings of Hershey to include determining whether a sum of the session length and a time stamp received as part of the authorization ticket is within a preset threshold value of a current time and that in

response to determining that the sum of the session length and the time stamp is within a preset threshold value, authorizing the client computer to access said second server-based application with the motivation to provide a highly fault tolerant method of relaying information to a desired communication unit (Hershey, col. 2, lines 53-54).

In regards to claim 15, Sasmazel teaches that in response to determining that the hash value received from the client computer is not identical to the new hash value, not authorizing said client computer to access said second server-based application (col. 9, lines 10-16), (col. 10, lines 25-27).

In regards to claim 16, the system of Sasmazel, Roberts and Misra does not teach that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value, it does not authorize the client computer to access the second server-based application.

Hershey teaches that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value (i.e. the message expired), it does not authorize the client computer to access the second server-based application (i.e. message packet is erased) (figure 5a, steps 57 and 49).

Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to further modify the system of Sasmazel, Roberts and Misra with the teachings of Hershey to include that in response to determining that the sum of the session length and the time stamp is not within a preset threshold value, it does not authorize the client computer to access the second server-based application with the motivation to provide a highly fault tolerant method of relaying information to a desired communication unit (Hershey, col. 2, lines 53-54).

In regards to claim 18, the claim limitation recites a computer-controlled apparatus operative to perform the method of claim 14, therefore the same rejection applies.

In regards to claim 20, the claim limitation recites a computer-readable medium containing computer-readable instructions which, when executed by a computer, perform the method of Claim 14, therefore the same rejection applies.

In regards to claim 21, Sasmazel teaches that the first server-based application comprises an instant messaging server computer (i.e. web server) and that the second server-based application comprises a Web server computer (figure 2).

Action is Final

5. **THIS ACTION IS FINAL**. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Conclusion

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Taghi T. Arani, Ph.D.
Examiner
Art Unit 2131

GILBERTO BARRON JR.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100